LeddarTech®

WHITE PAPER

Cybersecurity in ADAS: Protecting Connected and Autonomous Vehicles

Release Date: September 12, 2024

Abstract

July 2024: A cyberattack hits the airport in the coastal city of Split, Croatia, leading to several flight cancelations and delays, and forcing passengers to spend the night at the airport.

June 2024: Automotive software provider CDK Global suffers multiple cyberattacks, causing over 15,000 dealerships across North America to go offline.

June 2024: The Japanese government announces that its space agency becomes the target of a series of cyberattacks starting in 2023. Fortunately, the compromised network does not contain sensitive rocket or satellite information.

April 2024: Hackers attack El Salvador's national cryptocurrency wallet, Chivo, exposing the sensitive personal information of millions of Salvadorians. They also release Chivo's source code.

Cyberattacks across industries are on the rise[1]. Whether private or public, large or small, no business is immune to the threat of cyberattacks. The motivations of cyber attackers vary, ranging from ransomware

[1] As referenced in a Forbes article updated on Aug 28, 2024: Cybersecurity Statistics.

demands to the public release of private information. As the automotive industry moves towards a software-defined future, it is crucial to prioritize cybersecurity in the design and deployment of vehicles.

This White Paper explores the impact of cybersecurity on the automotive industry, focusing on software-defined vehicles, connected vehicles, advanced driver assistance systems (ADAS) and automated vehicles (AVs) as well as design practices that can be implemented to enhance cybersecurity.

Understanding Software-Defined Vehicles

Software-defined vehicles (SDVs) represent the future of automotive technology, where the functionality, performance, features and value are derived from the vehicle's software capabilities rather than its hardware, such as chassis, gearbox or engine. Today, traditional and new original equipment manufacturers (OEMs) are embracing the shift towards SDVs, offering users the ability to purchase features like adaptive cruise control (ACC), autopilot capabilities and adaptive headlights through a subscription service. SDVs come equipped with the necessary hardware to support these features when they leave the factory. When customers subscribe to the additional features, the vehicle is updated over-the-air (OTA), allowing them to enjoy their new capabilities without needing to visit a dealership.

SDVs are built on a foundation of advanced software platforms that can be updated, customized and optimized over time. This approach allows for continuous enhancement of vehicle features, such as ADAS, infotainment and even powertrain performance, without necessitating physical modifications to the vehicle. Software updates, often delivered over-the-air, enable manufacturers to introduce new features, fix bugs and improve security after the initial purchase, transforming the vehicle into a dynamic product that evolves throughout its lifecycle.

A modern car runs on over 100 million lines of code and 250 GB of data flowing through its system. It contains more than 1,500 wires stretching for miles. In comparison, vehicles produced in the early 2000s had significantly fewer software components and wiring, and those from the 1970s had even less. Given how central software has become in everyday life, it's no surprise that it has impacted the automotive industry. What is surprising, however, is that it has taken this long for software to become the key cornerstone.

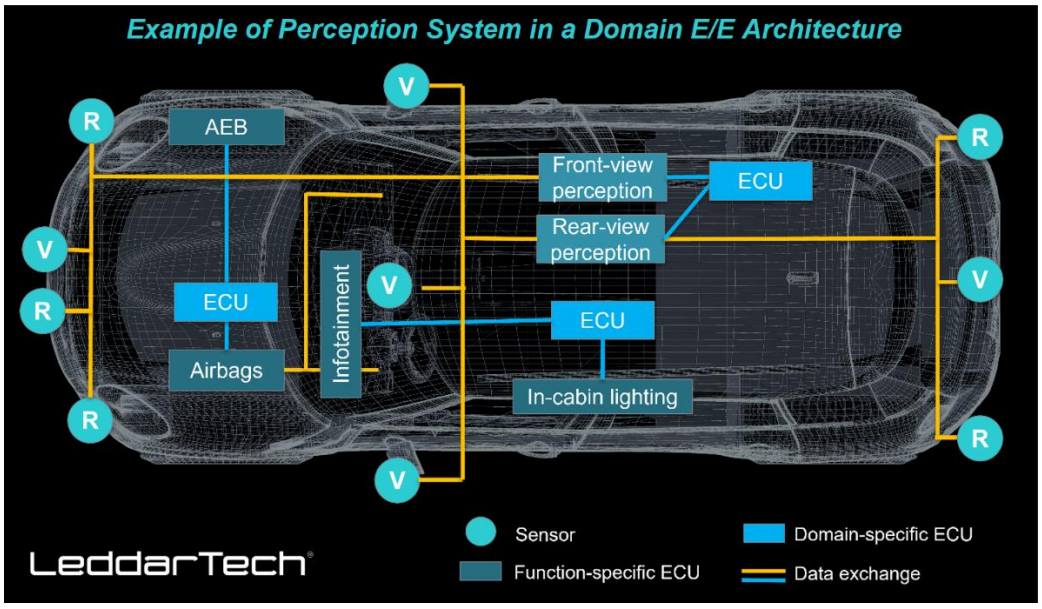


Figure 1 – Example of data exchange in a modern vehicle. Future SDVs will transform electrical/electronic design by adopting a zonal architecture.

Cybersecurity Challenges in Automotive

The automotive industry faces unique challenges not typically encountered by many software-based products. Automakers must comply with stringent safety requirements, integrate multiple systems from third-party suppliers over which they often have limited control, meet national and global regulatory standards and coordinate with dealerships to deliver the product to customers. Legacy automakers face additional challenges in transitioning to an SDV future due to the extensive technical baggage they carry. Having manufactured vehicles for decades, acquired companies and adopted various technology suites, these automakers must now find a way to design vehicles coherently and integrate multiple technical stacks seamlessly. Traditionally, vehicle design has been modular, featuring distinct domains such as chassis, infotainment, climate control and engine. However, the shift to SDVs necessitates a holistic design approach. New automakers, unburdened by legacy systems, can develop their SDVs on fewer technical platforms, enabling a more integrated approach to vehicle design and an enhanced customer experience.

Exceptional cybersecurity is crucial for automakers to successfully deploy SDVs. Car theft is increasing in many parts of North America and Europe, with one prevalent method being the relay attack[2]. In a relay attack, thieves use hand-held radio relays to extend the communication range between the car and its key. They first use one relay to capture the car's signal and transmit it to a second relay placed near the key. This second relay then sends the signal back to the car, causing it to unlock. The thieves can then steal the vehicle. As awareness of this method grew, car owners began storing their keys in metal boxes to block the signal. In response, thieves have developed new techniques.

In more modern vehicles, theft has been mitigated by pairing a smart key with the vehicle. This smart key exchanges cryptographic messages with the vehicle. When the vehicle requests authentication from the key, it requires a valid cryptographic response to unlock the car and disable the engine immobilizer. This advanced security measure helps to prevent unauthorized access and theft.

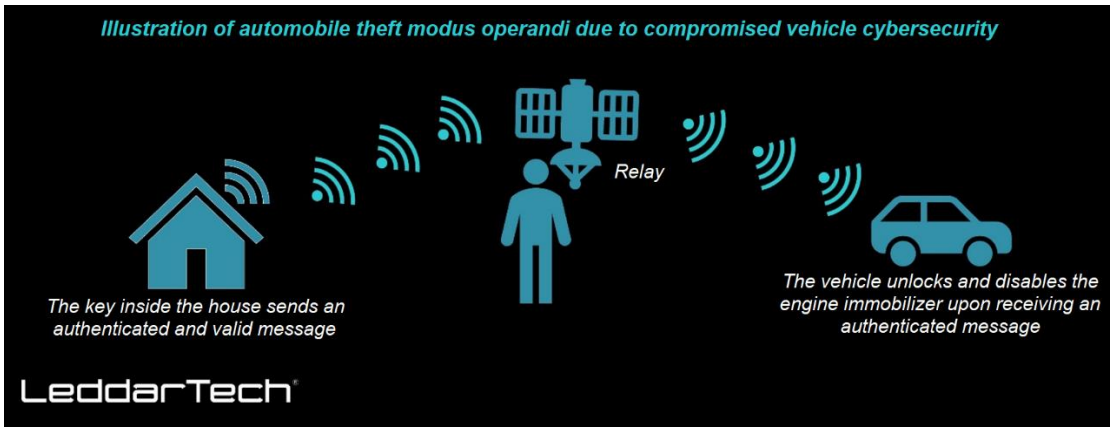


Figure 2 – Illustration of automobile theft resulting from inadequate cybersecurity measures

In response to the enhanced security features in modern vehicles, thieves have begun using CAN injection[3]. CAN, or Controller Area Network, is a communication protocol that allows various electronic control units (ECUs) within a vehicle to communicate with one another via a communication cable. CAN injection works as follows: Thieves gain access to the car's internal communication system, the CAN bus, and transmit fake messages that mimic those sent by the smart key. These false messages unlock the vehicle and disable the engine immobilizer. Most cars today do not verify the authenticity of internal CAN bus messages, allowing the vehicle to be stolen.

2 Ken Tindell, "Can Injection," Canis Automotive Labs, CTO Blog.

3 Zac Palmer, "Thieves are now stealing cars via a headlight CAN injection," Autoblog.

Cybersecurity in vehicles is essential because today's cars are increasingly connected and reliant on software to control critical systems such as braking, steering and ADAS. A cybersecurity breach could enable hackers to take control of these systems, potentially leading to accidents, car theft or even unauthorized surveillance. Additionally, vehicles may collect and transmit sensitive personal data, making them attractive targets for data breaches. Robust cybersecurity measures are essential not only for protecting the physical safety of drivers and passengers but also for safeguarding their privacy and maintaining consumer trust in the rapidly evolving automotive industry.

Most vehicles today are equipped with cameras, often multiple. As vehicles navigate roads and travel from point A to point B, they may capture images of people's faces. Ensuring that cars are not used for surveillance and protecting individuals' privacy and data are also key concerns for all stakeholders.

The implications of cybersecurity for autonomous vehicles and ADAS systems are extensive. A lack of cybersecurity in ADAS and autonomous driving (AD) systems can lead to devastating consequences, such as loss of vehicle control, incorrect navigation, being trapped inside the vehicle or accidents. To ensure that present and future vehicles are secure, the automotive industry has adopted standards and processes designed to manufacture products that are safe, secure and reliable.

Standards Applicable to ADAS and AD

While there are many standards applicable to various aspects of autonomous driving, this document highlights the following key standards:

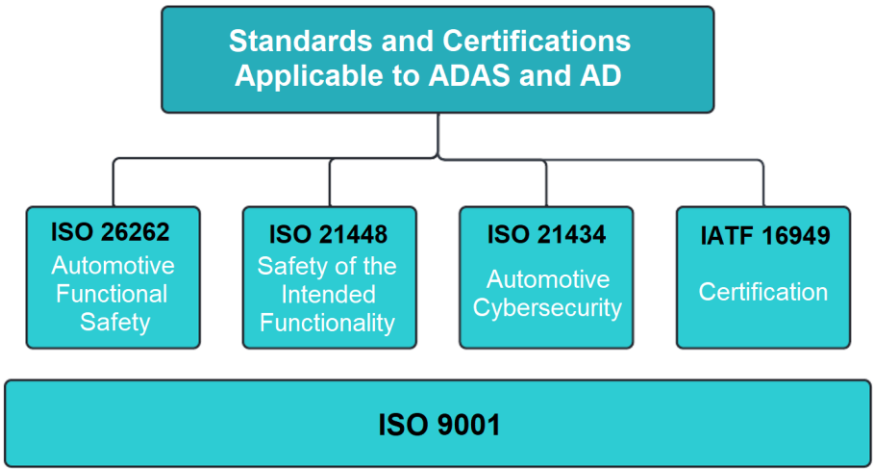


Figure 3 – Block diagram of standards and certifications applicable to ADAS and AD

- **ISO 26262 – Automotive Functional Safety (FuSA):** FuSA is a comprehensive approach to ensuring the electronic safety of vehicles. It aims to protect drivers, passengers and vulnerable road users (VRUs), including pedestrians, cyclists, motorcyclists and others, from injuries caused by faults in vehicle electronics and software.
- **ISO 21448 – Safety of the Intended Functionality (SOTIF):** SOTIF focuses on eliminating unreasonable risks caused by hazards resulting from functional inadequacies of the intended functionality or foreseeable misuse by individuals. ISO 21448 provides guidelines to help achieving this level of safety.
- **ISO 21434 – Automotive Cybersecurity:** This standard provides guidelines to enhance cybersecurity within the automotive industry and addresses issues such as:
  - Organizational and project-based cybersecurity management
  - Managing cybersecurity with suppliers

  - Cybersecurity throughout the product concept, development and production phases
  - Incident response, threat analysis and risk assessment
- **IATF 16949 – International Automotive Task Force:** IATF 16949 is an automotive quality management system standard focused on continual improvement. It emphasizes defect prevention and the reduction of variation in the automotive supply chain and assembly processes.

These standards are vital in the automotive industry as they provide frameworks for ensuring the safety and security of increasingly complex vehicles. In the context of this White Paper, ISO 21434 offers the most comprehensive set of guidelines for enhancing vehicle cybersecurity, covering everything from design and development to production and maintenance.

ISO 21434 ensures that manufacturers implement robust cybersecurity practices to protect against threats such as hacking, data breaches and unauthorized access, which could compromise vehicle safety and user privacy. This standard applies to various sub-systems within the vehicle, including connected vehicles, electronic systems, software, ADAS and AD, among others. It provides developers with the necessary knowledge to integrate cybersecurity measures throughout the development cycle and across the supply chain.

The standard is based on a risk-based approach, requiring manufacturers to systematically identify potential cybersecurity threats, assess their impact and implement appropriate mitigation measures. It encompasses, among other aspects, integrating cybersecurity into design and development to ensure that vehicles *are designed with security in mind*. ISO 21434 places a strong emphasis on continuous monitoring and the capacity for incident response, enabling timely detection and reaction to threats throughout the vehicle's lifecycle.

Furthermore, ISO 21434 establishes a foundation for cooperation among all automotive supply chain stakeholders, fostering the understanding that cybersecurity is a collective responsibility.

Cybersecurity will play an increasingly important role as the automotive industry moves towards a future dominated by software-defined vehicles. These vehicles, which offer over-the-air performance updates, bug fixes and the ability to unlock advanced driver assistance features, will require reliable suppliers who understand the importance of developing software solutions in compliance with the aforementioned standards, while balancing performance and cost challenges.

Cybersecurity for Vehicles with Advanced Driver Assistance Systems

Cybersecurity for vehicles with ADAS involves protecting electronic systems, communication networks, software and data from cyber threats and unauthorized access. ADAS features, such as adaptive cruise control (ACC), lane keep assist (LKA) and automatic emergency braking (AEB), rely on sensors, cameras, radar and complex software. The growing integration of these technologies introduces new cybersecurity challenges and potential vulnerabilities. Below is an overview of the key elements of cybersecurity for vehicles with ADAS:

1. **Protection of Communication Networks:** ADAS relies on various internal communication protocols, such as CAN (Controller Area Network), LIN (Local Interconnect Network) and Ethernet, alongside external communications like V2X (Vehicle-to-Everything). Safeguarding these communication channels from cyber threats –including man-in-the-middle attacks, spoofing and jamming– is essential for ensuring the security and functionality of the system.
2. **Sensor Security:** ADAS systems rely on sensors such as cameras, radar, LiDAR and ultrasonic sensors to interpret the vehicle's surroundings. Cyber attackers may target these sensors to feed false data, leading to incorrect decision making. Ensuring sensor data integrity through validation techniques and secure communication protocols is vital.

3. **Software Security and Secure Coding Practices:** ADAS functionalities are governed by complex software algorithms. Ensuring the use of secure coding practices, along with rigorous testing and vulnerability assessments, is essential to minimize the risk of software-based attacks. Regular updates and effective patch management are also critical for addressing newly discovered vulnerabilities and maintaining system security.
4. **Secure Software Updates (OTA):** Vehicles with ADAS can receive over-the-air (OTA) software updates. Ensuring these updates are securely delivered without being intercepted, modified or corrupted is crucial. Secure OTA mechanisms typically rely on encryption, digital signatures and authentication to safeguard the update process.
5. **Access Control and Authentication:** Strong access control measures are essential to ensure that only authorized users and devices can interact with the vehicle's ADAS features. This involves implementing multi-factor authentication, cryptographic keys and secure credentials for systems that interact with ADAS, preventing unauthorized access and manipulation.
6. **Intrusion Detection and Prevention Systems (IDPS):** Monitoring the vehicle's network and systems for signs of unauthorized access or malicious activity is requisite. IDPS can detect anomalies or potential cyberattacks in real time, allowing the system to initiate countermeasures that prevent or minimize damage.
7. **Data Privacy and Protection:** ADAS systems generate and process extensive data, including vehicle speed, location and other driver-specific information. Securing the storage, transmission and processing of this data is crucial for protecting user privacy and preventing data breaches.
8. **Firmware Integrity and Secure Boot:** Secure boot mechanisms are imperative for preventing malicious code from being executed within the vehicle's systems. These mechanisms verify the integrity of the firmware during startup, ensuring that only authorized and unaltered firmware is used.

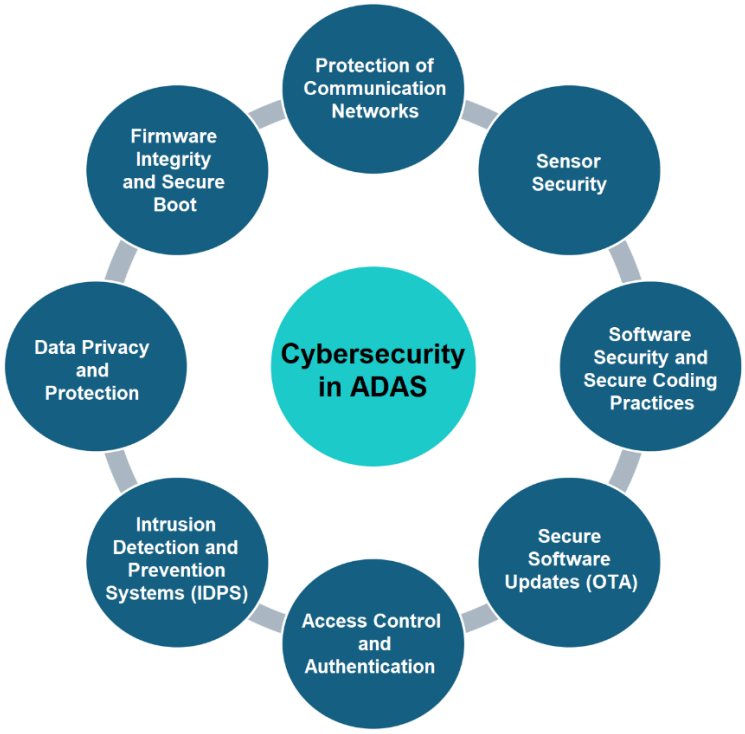


Figure 4 – Various aspects of cybersecurity in ADAS

Cybersecurity is fundamental for ADAS-enabled vehicles as it directly affects safety, reliability and regulatory compliance. Cyberattacks on these systems could lead to unauthorized control of crucial functions such as steering, braking or acceleration, posing significant risks to the driver, passengers and others on the road. Implementing robust cybersecurity measures contributes to maintaining the reliability of ADAS features, which is key to building public trust and encouraging user acceptance. As the adoption of these technologies increases, so does the necessity to comply with cybersecurity regulations and standards, which are becoming mandatory as governments and industry bodies recognize the importance of securing vehicle systems against potential threats. Failure to protect ADAS-equipped vehicles can result in severe consequences, including accidents, financial losses and legal liabilities, making cybersecurity a top priority for automakers and technology providers.

Overcoming Performance and Cost Challenges with LeddarTech

LeddarTech is a global software company founded in 2007 and headquartered in Quebec City, Canada, with additional R&D centers in Montreal and Tel Aviv (Israel). The company offers innovative AI-based low-level sensor fusion and perception technology for ADAS and AD. LeddarTech's technology generates a comprehensive 3D environmental model from various sensor types (including cameras, radar and LiDAR) and configurations. LeddarTech's flagship solution, LeddarVision™, meets numerous performance requirements, such as:

- Higher range
- Higher accuracy
- Fewer false alarms
- Superior object detection, including VRUs and occluded objects
- Small object detection

LeddarTech's cost-effectiveness can be realized in three key ways by automotive Tier 1 suppliers and vehicle manufacturers:

1. **Lower System Cost:** LeddarTech reduces the overall perception system cost by requiring fewer sensors compared to object-level fusion solutions. For example, while most surround-view solutions today use an 11-camera and 5-radar configuration, the LeddarVision Surround-View (LVS-2^{+}) utilizes a 5-camera and 5-radar configuration. With multiple sensors required for front-view or surround-view perception in each vehicle, the savings per vehicle can accumulate significantly across the millions of vehicles produced by automotive OEMs. According to LeddarTech's internal study and estimates based on market information, LeddarTech's Front-View solution (LVF-E) and Surround-View solution (LVS-2^{+}) are 44% and 48% more cost-effective, respectively, compared to their camera-centric counterparts.
2. **Lower Long-Term Costs:** LeddarTech's solutions are scalable, allowing the same platform to support L2 ADAS and scale up to higher levels of automated driving. This unified architectural approach minimizes rework with sensor changes and efficiently scales computational power with additional sensors needed for higher levels of ADAS and AD. Consequently, this scalability can significantly reduce R&D time, effort and financial investment for automotive Tier 1 suppliers and OEMs.
3. **Indirect Cost Savings:** Reducing sensor requirements not only offers direct cost benefits but also indirectly affects other system costs. Fewer sensors lead to lower processing costs, reduced heat management needs, and energy savings. In addition, reduced sensor count decreases wiring requirements and vehicle weight, resulting in lower electrical/electronic (E/E) costs.

This White Paper does not constitute a reference design. The recommendations contained herein are provided "as is" and do not constitute a guarantee of completeness or correctness.

LeddarTech® has made every effort to ensure that the information contained in this document is accurate. Any information herein is provided "as is." LeddarTech shall not be liable for any errors or omissions herein or for any damages arising out of or related to the information provided in this document. LeddarTech reserves the right to modify design, characteristics and products at any time, without notice, at its sole discretion.

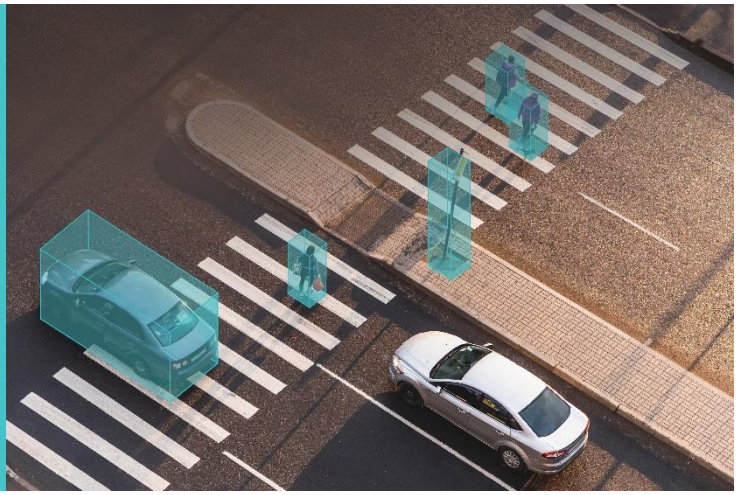
LeddarTech does not control the installation and use of its products and shall have no liability if a product is used for an application for which it is not suited. You are solely responsible for (1) selecting the appropriate products for your application, (2) validating, designing and testing your application and (3) ensuring that your application meets applicable safety and security standards.

Furthermore, LeddarTech products are provided only subject to LeddarTech's Sales Terms and Conditions or other applicable terms agreed to in writing. By purchasing a LeddarTech product, you also accept to carefully read and to be bound by the information contained in the User Guide accompanying the product purchased.

About LeddarTech

A global software company founded in 2007 and headquartered in Quebec City with additional R&D centers in Montreal and Tel Aviv, Israel, LeddarTech develops and provides comprehensive AI-based low-level sensor fusion and perception software solutions that enable the deployment of ADAS, autonomous driving (AD) and parking applications. LeddarTech's automotive-grade software applies advanced AI and computer vision algorithms to generate accurate 3D models of the environment to achieve better decision making and safer navigation. This high-performance, scalable, cost-effective technology is available to OEMs and Tier 1-2 suppliers to efficiently implement automotive and off-road vehicle ADAS solutions. LeddarTech is responsible for several remote-sensing innovations, with over 160 patent applications (87 granted) that enhance ADAS, AD and parking capabilities. Better sensory awareness of the environment around the vehicle is critical in making global mobility safer, more efficient, sustainable and affordable: this is what drives LeddarTech to seek to become the most widely adopted sensor fusion and perception software solution.

For more information: sales@leddartech.com



LeddarTech®

CANADA – USA – AUSTRIA – FRANCE – GERMANY – ITALY – ISRAEL – HONG KONG – CHINA

Head Office
4535, boulevard Wilfrid-Hamel, Suite 240
Québec (Québec) G1P 2J7, Canada
leddartech.com

Phone: + 1-418-653-9000
Toll-free: 1-855-865-9900